REPORT DOCUMENTATION PAGE	Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 17-10-2009	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 20-May-2005 - 19-Aug-2008

4. TITLE AND SUBTITLE QA - Research on Quantum Algorithms at the Institute for Quantum Information	5a. CONTRACT NUMBER W911NF-05-1-0294
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER 0BXXX1
6. AUTHORS Alexei Kitaev, John Preskill, Leonard Schulman	5d. PROJECT NUMBER 0BXXX1
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES California Institute of Technology Sponsored Research MC 201-15 California Institute of Technology Pasadena, CA 91125 -	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S. Army Research Office P.O. Box 12211 Research Triangle Park, NC 27709-2211	10. SPONSOR/MONITOR'S ACRONYM(S) ARO 11. SPONSOR/MONITOR'S REPORT NUMBER(S) 47971-PH-QC.1

12. DISTRIBUTION AVAILIBILITY STATEMENT

Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

The central goals of our project are (1) to bring large-scale quantum computers closer to realization by proposing and analyzing new schemes for protecting quantum systems from noise, and (2) to conceive, develop, and analyze new applications of quantum computing to physics and mathematics. We proved quantum threshold theorems for long-range correlated non-Markovian noise, for leakage faults, for the one-way quantum computer, for postselected quantum computation, and for biased noise. We showed that quantum algorithms can speed up the evaluation of

15. SUBJECT TERMS

quantum algorithms, fault-tolerant quantum computation, quantum simulation

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			John Preskill
U	U	U	SAR		19b. TELEPHONE NUMBER 626-395-6691

Final Report
Research on Quantum Algorithms at the Institute for Quantum Information

Principal Investigators: John Preskill, Alexei Kitaev, Leonard Schulman (Caltech)

Postdoctoral Associates: Robin Blume-Kohout, Andrew Childs, Robert Koenig, Yi-Kai Liu, David Poulin, Robert Raussendorf, Ben Reichardt, Stephanie Wehner, Pawel Wocjan, Jon Yard, Shengyu Zhang

Graduate Students: Anura Abeyesinghe, Panos Aliferis, Ersen Bilgin, Parsa Bonderson, Peter Brooks, Kovid Goyal, Isaac Kim, Prabha Mandayam, Hui Khoon Ng, Graeme Smith, Benjamin Toner, Greg ver Steeg, Michael Zwolak

Type of Award: QA

Start Date: May 20, 2005
End Date: May 19, 2008

Report Date: October 2009

Main Project Goals:
The central goals of our project are (1) to bring large-scale quantum computers closer to realization by proposing and analyzing new schemes for protecting quantum systems from noise, and (2) to conceive, develop, and analyze new applications of quantum computing to physics and mathematics.

Project Description:
This project is devoted to building the theoretical foundations of quantum information science across a broad front, with a particular emphasis on quantum algorithms, quantum complexity, and fault-tolerant quantum computing. Basic advances in all of these areas are needed to bring revolutionary quantum technologies closer to realization. The research is conducted at Caltech's Institute for Quantum Information (IQI).

Our research on fault-tolerant quantum computing addresses the crucial questions: How much noise can be tolerated by a quantum computer, and how does the noise impact the resources needed to complete a large-scale computation successfully? It is vital to answer these questions to assess the prospects for realizing powerful quantum technologies. Our approach emphasizes rigorous results. We also pursue new ways to encode and process quantum information that are intrinsically robust on physical grounds.

Our research on quantum algorithms emphasizes new applications that reach beyond the hidden subgroup paradigm. Topics of particular interest include algorithms based on quantum walks, novel applications of the Fourier transform and other quantum transforms, and simulations of quantum many-body systems using quantum or classical computers.

Status and Accomplishments 2005-08 (incomplete list):
Our research covered four broad categories: (1) The search for new quantum algorithms, e.g., going beyond the hidden subgroup problem. (2) Quantum nonlocality, quantum cryptography, quantum communication, e.g., channel capacities, and secret key rates. (3) Fault-tolerant quantum computing, with emphasis on rigorous results. (4) Simulation of quantum systems with classical and quantum computers. What follows is an incomplete list of our accomplishments.

Papers in 2005-06:
Quantum threshold theorem for correlated noise: Aharonov, Kitaev, and Preskill found a new proof of the quantum accuracy threshold theorem that applies to non-Markovian noise with algebraically decaying spatial correlations. The proof shows that an arbitrarily long quantum computation can be executed with high reliability in D spatial dimensions, if the perturbation is sufficiently weak and decays with the distance r between the qubits faster than $1/r^D$.

Threshold theorem for one-way quantum computer: Raussendorf, Goyal, and Harrington proved a quantum accuracy threshold theorem for the one-way quantum computer. Their proof is based on a novel scheme, in which a noisy cluster state in three spatial dimensions is transformed to a high-fidelity topologically encoded two-dimensional cluster state; concatenated quantum codes protect the non-Clifford gates in a universal fault-tolerant gate set.

Fault-tolerance against leakage: Aliferis and Terhal rigorously analyzed fault-tolerant quantum computation in the presence of local leakage faults, and proved a quantum accuracy threshold theorem that covers this case. Their proof adapts the methods developed earlier by Aliferis, Gottesman, and Preskill to encompass leakage-reduction units, such as those based on quantum teleportation. They also described how to optimize the overhead cost of leakage reduction, and showed that measurement-based computation is inherently tolerant against leakage faults.

Quantum computing with quantum Hall states: Bravyi developed the theory of quantum computation using nonabelian anyons, and explained how to achieve universal quantum computation in the simplest realistic model --- the Pfaffian state realized in fractional quantum Hall systems at electron filling factor nu=5/2. Using distillation schemes for magic states that he had proposed earlier with Kitaev, Bravyi showed that one rather noisy nontopological gate, together with the topological gates, suffices for computational universality. Assuming that all topological operations are implemented perfectly, he proved that the threshold error rate for non-topological operations is above 14%, and that the total number of non-topological computational operations needed to simulate a quantum circuit with L gates scales as $L(\log L)^3$.

Proposed experimental probe of nonabelian anyons: Bonderson, Kitaev, and Shtengel proposed an interferometric test of non-Abelian statistics in fractional quantum Hall systems, that would provide the first proof of principle in the lab of one of the primitive elements of a topological quantum computer. This paper set in motion an intense race to confirm the predicted experimental signal, as is featured in the Search and Discovery section of the October 2005 Physics Today and in the April 2006 Scientific American.

Topological entanglement entropy: Kitaev and Preskill discovered a new type of universal ``topological quantum entanglement" that arises in topologically ordered gapped two-dimensional media. Using methods borrowed from topological quantum field theory, they found a formula for the entropy that characterizes this topological entanglement, in terms of the properties of the superselection sectors of the medium.

Time required to establish topological order: Bravyi, Hastings, and Verstraete obtained lower bounds on the time required to establish quantum correlations under local Hamiltonian evolution. Using the Lieb-Robinson bound, which establishes an effective light cone with exponentially decaying tails, they showed that there is a finite speed at which correlations and entanglement can be distributed. They also proved lower bounds on the time it takes to convert states without topological quantum order to states with that property, and showed that the rate at which entropy can be created in a block of spins scales with the boundary of that block.

Hardness of hidden shift problem: Childs and Wocjan argued that it is more natural to approach the graph isomorphism problem as a hidden shift problem, instead of the more standard view of regarding it as a hidden subgroup problem. However, they concluded that the problem is still hard when approached in this way, in two senses: (1) Omega(n) copies of the hidden shift state are necessary to solve the problem efficiently (where n is the number of vertices in the graph), and (2) if one is restricted to single-register measurements, then an exponential (in n) number of hidden shift states are required.

Quantum k-SAT: Bravyi formulated a quantum analogue of the satisfiability problem ("quantum k-SAT"), and showed that quantum 2-SAT can be solved efficiently by a classical computer. He also showed that for k > 3 quantum k-SAT is a complete problem for the complexity class QMA with one-sided error. Quantum k-SAT is the problem of determining whether an n-qubit pure state exists whose k-qubit reduced density matrices have support on prescribed subspaces.

Quantum algorithms for knot invariants: Wocjan and Yard found new quantum algorithms for approximating the evaluations of knot polynomials. Their polynomial-time algorithm achieves an additive approximation at any primitive root of unity to the Jones polynomial for links obtained from a general type of closure of a braid, generalizing recent results of Aharonov, Jones and Landau, and also provides an additive approximation to the HOMFLYPT two-variable polynomial of the trace closure of a braid, evaluated at certain pairs of points. They also found self-contained proofs that a quantum computation can be simulated by an approximate evaluation of the Jones polynomial, that evaluating the Jones polynomial is #P-hard, and that learning its most significant bit is PP-hard, and they formulated QCMA-complete and PSPACE-complete problems based on braids.

Correlations compatible with lack of superluminal signaling: Toner derived upper bounds on the correlations in a bipartite physical system that follow only from the requirement that superluminal signaling is impossible, without assuming the validity of quantum mechanics. He also showed that in a tripartite system ABC, forcing classical correlations between B and C prevents A and B from violating certain Bell inequalities. These results can be applied to find proofs of security for cryptographic protocols, assuming only the impossibility of superluminal signaling.

Private key from twisted states: Graeme Smith, with Renes, found a new method for analyzing the security of quantum key distribution protocols that employ noisy preprocessing and one-way postprocessing of the key. They showed that the security of the protocol is equivalent to that of an associated key distribution protocol in which, instead of the usual maximally-entangled states, a more general type of private state called a twisted state is distilled. The noisy preprocessing allows some phase errors to be left uncorrected without compromising the privacy of the key, thus improving the rate at which secure final key can be extracted

Papers in 2006-07:

Quantum algorithms for hidden nonlinear structures: Childs and Schulman, with Vazirani, studied the quantum complexity of finding hidden nonlinear structures. They found two black-box problems involving spheres over finite fields for which a classical computer requires exponentially many queries, but a quantum computer can solve the problem in polynomial time. These results show that abelian Fourier sampling is applicable to algebraic structures other than groups, suggesting a new way to generalize the abelian hidden subgroup problem solved by Shor's algorithm.

Quantum speedup for arbitrary Boolean formulas: Childs, Reichardt, and Zhang, with Spalek, generalized the algorithm of Farhi, Goldstone, and Gutmann to arbitrary Boolean formulas written in terms of NAND gates. In general, such formulas can be evaluated using only $O(N^{1/2+o(1)})$ queries, nearly matching the $O(N^{1/2})$ lower bound of Barnum and Saks.

Accuracy threshold for postselected quantum computation: Preskill and Panos Aliferis, with Gottesman, proved an accuracy threshold theorem for fault-tolerant quantum computation based on error detection and postselection. Their proof provides a rigorous foundation for the scheme suggested by Knill, in which preparation circuits for ancilla states are protected by a concatenated error-detecting code and the preparation is aborted if an error is detected. The proof applies to independent stochastic noise but (in contrast to proofs of the quantum accuracy threshold theorem based on concatenated error-correcting codes) not to strongly-correlated adversarial noise. Their rigorously established lower bound on the accuracy threshold, 1.04×10^{-3}, is the highest proved so far.

Fault-tolerant quantum computing using subsystem codes: Aliferis, with Cross, analyzed fault-tolerant quantum computing based on sub-system codes; that is, codes with an unfixed gauge freedom. They observed that for the “Bacon-Shor code” the gauge freedom leads to a highly efficient method for fault-tolerant error correction that can be implemented using only nearest-neighbor two-qubit measurements. Using this method, they proved a lower bound on the accuracy threshold, 1.9×10^{-4} for adversarial stochastic noise, that improves previous lower bounds by almost an order of magnitude.

Topological fault-tolerance in cluster state quantum computation: Goyal and Raussendorf, with Harrington, extended their fault-tolerant scheme for the one-way quantum computer. In their scheme, topologically protected quantum gates are realized by choosing appropriate boundary conditions on a three-dimensional cluster state. The spatial dimensionality of the scheme can be reduced to two by converting one spatial axis of the cluster into time.

Optimal and efficient decoding of concatenated quantum block codes: Poulin considered the problem of optimally decoding a quantum error correction code (finding the optimal recovery procedure given the measured values of check operators). In general, this problem is NP-hard. However, he demonstrated that for concatenated block codes, the optimal decoding can be efficiently computed using a message passing algorithm. Monte Carlo results for the five-qubit and seven-qubit codes demonstrate that the message passing algorithm has a significantly higher error threshold and a significantly better rate compared to previously used decoding methods.

Quantum belief propagation: Poulin, with Leifer, developed a theory of quantum graphical networks, and a quantum belief propagation algorithm that solves inference problems on these networks. These generalize to the quantum setting the belief propagation algorithms that have found many applications classically, such as decoding error-correcting codes and characterizing the properties of disordered spin systems. They have also characterized the domain of exact convergence for their algorithm. These methods can be applied to decoding of quantum error-correcting codes and to simulation of quantum many-body systems.

Protected qubit based on a superconducting current mirror: Kitaev proposed a qubit implementation based on exciton condensation in capacitively coupled Josephson junction chains. In his proposal, the qubit is protected in the sense that all unwanted terms in its effective Hamiltonian are exponentially suppressed as the chain length increases. He also described an implementation of a universal set of quantum gates. Most of these gates have exponential error suppression; the only gate that is not intrinsically fault-tolerant needs to be realized with about 50% precision, provided the other gates are exact.

N-representability is QMA-complete: Verstraete, with Liu and Christandl, studied the computational complexity of N-representability, a central problem in quantum chemistry. They showed that this problem is QMA-complete, the quantum generalization of NP-complete. Their proof uses a simple mapping from spin systems to fermionic systems, as well as a convex optimization technique that reduces the problem of finding ground states to N-representability. The result strongly indicates that widely used methods for quantum chemistry computations on classical computers are not scalable.

Papers in 2007-08:

Span-program-based quantum algorithm for evaluating formulas: Reichardt, with Spalek, gave a quantum algorithm for evaluating “span programs” (a span program is a certain linear-algebraic way of specifying a classical function). In particular, the algorithm optimally evaluates balanced formulas over an extended gate set including all two-bit and three-bit gates (such as NAND and 3-majority). The main new tool in their analysis is a correspondence between span programs and weighted bipartite graphs --- a span program's evaluation corresponds to an eigenvalue-zero eigenvector of the associated graph. A quantum computer evaluates the span program by applying spectral estimation to the graph.

Wavefunction preparation using a quantum computer: Kitaev and Webb described a set of algorithms for preparing certain quantum states (representing continuous functions) on qubit ensembles. In particular, they presented an algorithm that prepares an ensemble of qubits into a wavefunction corresponding to a multidimensional Gaussian. This algorithm uses a very simple subroutine to prepare a set of independent one-dimensional Gaussian states and then employs a reversible transformation to produce an arbitrary Gaussian. These Gaussian states have applications in multidimensional resampling, where wavepacket stretching and squeezing is simulated using a fixed grid. This research is part of a broader effort to develop techniques for digital simulation on quantum computers.

Optimal quantum adversary lower bounds for ordered search: Childs, with Lee, found the exact value of the best possible quantum adversary lower bound for a symmetrized version of ordered search. The goal of the ordered search problem is to find a particular item in an ordered list of n items, and the query complexity of the symmetrized version differs from that of the unsymmetrized version by at most 1. They showed that the best lower bound for ordered search that can be proved by the adversary method (even if negative weights are allowed) is $(1/\pi) \ln n + O(1)$.

The complexity of the Local Consistency problem: Local Consistency is the qubit version of the N-representability problem in quantum chemistry. Liu found a novel reduction from Local Consistency to Local Hamiltonian, using strong duality of semidefinite programs. This reduction differs from previous work in that it preserves the structure of the underlying physical system. This allows one to study special classes of physical systems, such as 1-D and "stoquastic" systems, which are not necessarily QMA-hard; Liu found that Local Consistency and Local Hamiltonian still have equivalent complexity in these special cases.

Hardness of a single-shot energy measurement of a product state in a translation-invariant spin chain: Wocjan and Zhang, with Janzing, showed that the output of an arbitrary quantum circuit can be determined by performing a single-shot energy measurement on a computational basis state, where the energy is determined by the Hamiltonian of a one-dimensional qudit chain. Thus such energy measurements are as hard as the realization of any quantum computation. Here a "measurement" is a procedure that samples from the spectral measure induced by the observable and the state under consideration (the post-measurement state is irrelevant), and the required measurement accuracy scales inverse polynomially with the size of the simulated quantum circuit.

Lower bound methods for quantum one-way communication complexity: Communication complexity is a powerful tool for deriving lower bounds in numerous areas of classical theoretical computer science, which raises the fundamental question: how large is the gap between the classical and quantum communication complexity for evaluation of total functions? The answer remains elusive, despite much effort. Shengyu Zhang showed that all the known quantum lower bound methods for the one-way communication model can be exponentially weak, explaining past failures to settle the question, and highlighting the need for new lower bound methods. Then, with Jain, Zhang derived new lower bounds for quantum one-way distributional communication complexity in terms of a widely-used measure, the rectangle bound. They also derived new *upper* bounds for classical one-way communication complexity in terms of mutual information in a hard distribution, improving on the best known previous results for total functions.

Making classical honest-verifier zero-knowledge protocols secure against quantum attacks:

Zhang, with Hallgren, Kolla, and Sen, showed that any classical Statistical Zero-Knowledge protocol can be modified such that the resulting protocol is still secure, yet is provably secure against any quantum attack. In a Zero-Knowledge proof system, the Prover convinces the Verifier that a statement is true without revealing any further information to the Verifier beyond the validity of the statement. Zero-Knowledge is a well-studied area in theoretical computer science and cryptography, and Zhang's work establishes a particular setting where classical cryptographic protocols can retain their power even in the post-quantum world.

Sampling of min-entropy relative to quantum knowledge: Koenig, with Renner, showed that quantum conditional min-entropy is preserved under random sampling of subsystems. This generalizes a result previously shown in a purely classical context by Vadhan. It implies that the sample-then-hash approach for generating keys in the bounded storage model is secure even in the presence of a quantum adversary. The proof relies on a novel decomposition of conditional density operators which might have further applications in single-shot quantum information theory.

Cryptography from noisy photonic storage: Wehner, with Schaffner and Terhal, showed that cryptographic tasks can be implemented securely based on the assumption that it is difficult to store quantum states without errors. They considered an explicit noise model inspired by present-day technology, allowing the adversary to extract a noisy record of each incoming qubit, and derived explicit security tradeoffs between the amount of noise that occurs when storing quantum states and the amount of noise the honest parties experience when sending qubits over a channel. They concluded that security can be achieved if the channel noise rate does not exceed 11% and is strictly smaller than the storage noise rate. They devised protocols that realize secure oblivious transfer and also secure identification (where a party identifies herself without giving away her password).

Quantum graphical models and belief propagation: Poulin, with Leifer, generalized the concept of graphical models to the quantum setting. Classical graphical models are used to describe a wide variety of inference problems and have applications in numerous scientific fields. Poulin and Leifer proposed a generalized belief propagation algorithm suited for quantum graphical models and characterized its domain of applicability. They also applied the algorithm to the problem of decoding quantum error-correcting codes and to computing correlations of many-body quantum systems.

On exchangeable continuous variable systems: Koenig, with Wolf, studied permutation-invariant Gaussian states and their partial traces, i.e., exchangeable Gaussian states. They gave a complete characterization of the corresponding covariance matrices and derived bounds on the approximation of Gaussian exchangeable states by convex combinations of product states. This result extends de Finetti-type arguments to an important class of states of infinite-dimensional systems.

The quantum moment problem and bounds on entangled multi-prover games: Wehner, with Doherty, Liang, and Toner, studied the quantum moment problem: Given a conditional probability distribution, does there exist a quantum state and a collection of measurement operators compatible with the distribution and with a specified set of polynomial constraints?

Using recent results from algebraic geometry, they showed that if an instance of the quantum moment problem is unsatisfiable, then there exists a certificate of a particular form that proves unsatisfiability. They applied this result to one-round multi-prover games with entangled provers, showing that a hierarchy of semidefinite programs converges to the entangled value of the game (assuming that the Hilbert space shared by the provers is finite dimensional).

Fault-tolerant quantum computation against biased noise: Preskill, with Aliferis, formulated a scheme for fault-tolerant quantum computation that works effectively against highly biased noise, where phase errors in the computational basis are much more likely than bit-flip errors. In their scheme, the fundamental operations performed by the quantum computer are single-qubit preparations, single-qubit measurements, and conditional-phase (CPHASE) gates, where the noise in the CPHASE gates is biased; they showed that the accuracy threshold for quantum computation can be improved by exploiting the noise asymmetry. For example, if dephasing dominates bit-flip noise in the CPHASE gates by four orders of magnitude, they found a rigorous lower bound on the accuracy threshold higher by nearly a factor of five than for the case of unbiased noise.

Iterative decoding of sparse quantum codes: Poulin, with Chung, studied the problem of decoding a sparse quantum error-correcting code with an iterative algorithm, using techniques similar to those that yield state-of-the-art results for decoding classical codes. Unfortunately, the degeneracy of sparse quantum codes badly degrades the performance of the decoding algorithm. Poulin and Chung proposed some methods for overcoming this limitation, which, according to numerical simulations, greatly improve the performance.

Quantum serial turbo-codes: Poulin, with Tillich and Ollivier, presented a theory of quantum turbo-codes and studied their performance numerically for the case of a depolarizing channel. They demonstrated that, in contrast to the classical case, all recursive encoders lead to catastrophic error propagation. This important new feature of the theory leads to new code constructions and methods of analysis. The numerical results indicate that quantum turbo-codes are the best quantum error-correcting codes found to date, in terms of error threshold for a given transmission rate.

Topological cluster state quantum computing in three dimensions: Goyal, with Fowler, used the stabilizer formalism to reformulated and reanalyze protocols for fault-tolerant ``one-way'' quantum computation using three-dimensional cluster states. Their new analysis confirmed the principal conclusions found earlier by Goyal with other collaborators, specifically a threshold error rate approaching 1% and arbitrarily long-range logical gates with low overhead. Furthermore, this analysis applies to a broader range of quantum computing technologies.

Belief propagation algorithms for quantum many-body physics: Poulin and Bilgin have numerically investigated the performance of quantum belief propagation for the computation of correlation functions of finite-temperature quantum many-body systems on loopy graphs. Previously proposed efficient algorithms for this task (such as the density-matrix renormalization group method) work only for tree graphs. But in the classical setting, belief propagation is reliable on graphs with loops provided all the loops are large, and thus has been applied successfully to important problems in coding theory and statistical physics. The results of Poulin and Bilgin indicate that quantum belief propagation also works effectively for graphs that do contain small loops.

The structure of preserved information in quantum processes: Blume-Kohout, Poulin, and Hui Khoon Ng, with Viola, introduced a general characterization of information-preserving structures --- including noiseless subsystems, decoherence-free subspaces, pointer bases, and error-correcting codes --- in terms of the fixed points of quantum processes. They proved that the fixed states and observables of an arbitrary process are linearly isomorphic to a matrix algebra, which unifies the Schrodinger and Heisenberg pictures and rules out unphysical kinds of information. They also constructed a simple algorithm for efficiently finding all noiseless as well as unitarily noiseless subsystems.

Publications

D. Aharonov, A. Kitaev, and J. Preskill, Fault-tolerant quantum computation with long-range correlated noise, Phys. Rev. Lett. 96 050504 (2006).

S. Bravyi, Universal Quantum Computation with the nu=5/2 Fractional Quantum Hall State, Phys. Rev. A 73, 042313 (2006).

S. Bravyi, M. Hastings, and F. Verstraete, Lieb-Robinson bounds and the generation of correlations and topological quantum order, Phys. Rev. Lett. 97, 050401 (2006).

A. Kitaev and J. Preskill, Topological entanglement entropy, Phys. Rev. Lett. 96 110404 (2006).

P. Bonderson, A. Kitaev, and K. Shtengel, Detecting Non-Abelian Statistics in the nu=5/2 Fractional Quantum Hall State, Phys. Rev. Lett. 96, 016803 (2006).

P. Bonderson, K. Shtengel, and J. Slingerland, Probing Non-Abelian Statistics with QuasiParticle Interferometry, Phys. Rev. Lett. 97, 016401 (2006).

A. Childs and P. Wocjan, On the quantum hardness of solving isomorphism problems as nonabelian hidden shift problems, arXiv: quant-ph/0510185 (2005).

J. Yard and P. Wocjan, The Jones polynomial: quantum algorithms and applications in quantum complexity theory, arXiv: quant-ph/0603069 (2006).

J. Yard, P. Hayden, and I. Devetak, Quantum broadcast channels, arXiv: quant-ph/0603098 (2006).

J. M. Renes and Graeme Smith, Noisy preprocessing and the distillation of twisted states, arXiv: quant-ph/0603262 (2006).

D. Leung and G. Smith, Communicating over adversarial quantum channels using quantum list codes, arXiv: quant-ph/0605086 (2006).

G. Smith and J.~A. Smolin, Degenerate coding for Pauli channels, arXiv: quant-ph/0604107 (2006).

G. Smith and D. Leung, Typical entanglement of stabilizer states, arXiv: quant-ph/0510232 (2005).

B. Toner, Monogamy of nonlocal quantum correlations, arXiv: quant-ph/0601172 (2006).

R. Raussendorf, J. Harrington, and K. Goyal, A fault-tolerant one-way quantum computer, arXiv: quant-ph/0510135 (2005).

P. Aliferis and B. M. Terhal Fault-tolerant quantum computation for local leakage faults, arXiv: quant-ph/0511065 (2005).

Andrew M. Childs, Leonard J. Schulman, Umesh V. Vazirani, Quantum algorithms for hidden nonlinear structures, arXiv:0705.2784.

Andrew M. Childs, Ben W. Reichardt, Robert Spalek, Shengyu Zhang, Every NAND formula on N variables can be evaluated in time $O(N^{1/2+o(1)})$, arXiv:quant ph/0703015.

Andrew M. Childs, Aram W. Harrow, Pawel Wocjan, Weak Fourier-Schur sampling, the hidden subgroup problem, and the quantum collision problem, arXiv:quant-ph/0609110.

Andrew M. Childs, Andrew J. Landahl, Pablo A. Parrilo, Improved quantum algorithms for the ordered search problem via semidefinite programming, Phys. Rev. A 75, 032335 (2007), arXiv:quant-ph/0608161.

David Poulin, Jon Yard, Dynamics of a quantum reference frame, New Journal of Physics, to appear, arXiv:quant-ph/0612126.

Hoi-Kwong Lo, John Preskill, Security of quantum key distribution using weak coherent states with nonrandom phases, Quantum Information and Computation 7, 431-458 (2007), arXiv:quant-ph/0610203.

Robin Blume-Kohout, Hui Khoon Ng, David Poulin, Lorenza Viola, The structure of preserved information in quantum processes, arXiv:0705.4282.

Panos Aliferis, Daniel Gottesman, John Preskill, Accuracy threshold for postselected quantum computation, Quantum Information and Computation (accepted), arXiv:quant-ph/0703264.

Panos Aliferis, Andrew W. Cross, Sub-system fault tolerance with the Bacon-Shor code, Phys. Rev. Lett. 98, to appear (2007), arXiv:quant-ph/0610063.

David P. DiVincenzo, Panos Aliferis, Title: Effective fault-tolerant quantum computation with slow measurements, Phys. Rev. Lett. 98, 020501 (2007), arXiv:quant-ph/0607047.

Robert Raussendorf, Jim Harrington, Kovid Goyal, Topological fault-tolerance in cluster state quantum computation, arXiv:quant-ph/0703143.

David Poulin, Optimal and efficient decoding of concatenated quantum block codes, Phys. Rev. A, 052333 (2006), arXiv:quant-ph/0606126.

Alexei Kitaev, Protected qubit based on a superconducting current mirror, arXiv:cond-mat/0609441.

Yi-Kai Liu, Matthias Christandl, Frank Verstraete, N-representability is QMA-complete, Phys. Rev. Lett. 98, 110503 (2007), arXiv:quant-ph/0609125.

Dmitri E. Feldman, Alexei Kitaev, Detecting non-Abelian statistics with electronic Mach-Zehnder interferometer, Phys. Rev. Lett. 97, 186803 (2006), arXiv:cond-mat/0607541.

D. E. Feldman, Yuval Gefen, Alexei Kitaev, K. T. Law, Ady Stern, Shot noise in anyonic Mach-Zehnder interferometer, arXiv:cond-mat/0612608.

Parsa Bonderson, Kirill Shtengel, Joost Slingerland, Decoherence of anyonic charge in interferometry measurements, Phys. Rev. Lett. 98, 070401 (2007), arXiv:quant-ph/0608119.

Adrian Feiguin, Simon Trebst, Andreas W. W. Ludwig, Matthias Troyer, Alexei Kitaev, Zhenghan Wang, Michael H. Freedman, Interacting anyons in topological quantum liquids: The golden chain, Phys. Rev. Lett. 98, 160409 (2007), arXiv:cond-mat/0612341.

Ben W. Reichardt, Robert Spalek, Span-program-based quantum algorithm for evaluating formulas, Proc. Symp. on Theory of Computing (STOC) 2008, arXiv:0710.2630.

Alexei Kitaev, William A. Webb, Wavefunction preparation using a quantum computer, arXiv:0801.0342.

Andrew M. Childs, Troy Lee, Optimal quantum adversary lower bounds for ordered search, arXiv:0708.3396.

Yi-Kai Liu, The complexity of the consistency and N-representability problems for quantum states, arXiv:0712.3041.

Yi-Kai Liu, The Local Consistency problem for stoquastic and 1-D quantum systems, arXiv:0712.1388.

Dominik Janzing, Pawel Wocjan, Shengyu Zhang, A single-shot measurement of the energy of product states in a translation invariant spin chain can replace any quantum computation, arXiv:0710.1615.

Shengyu Zhang, On the power of lower bound methods for one-way communication complexity, submitted, 2008.

Rahul Jain, Shengyu Zhang, New bounds on classical and quantum one-way communication complexity, arXiv:0802.4101.

Andrew Childs, Universal computation by quantum walk, arXiv:0806.1972.

Sean Hallgren, Alexandra Kolla, Pranab Sen, Shengyu Zhang, Making classical honest verifier zero knowledge protocols secure against quantum attacks, Proceedings of the 35th International Colloquium on Automata, Languages and Programming (ICALP), 2008.

Robert Koenig, Renato Renner, Christian Schaffner, The operational meaning of min- and max-entropy, arXiv:0807.1338.

Christian Schaffner, Barbara Terhal, Stephanie Wehner, Robust cryptography in the noisy-quantum-storage model, arXiv:0807.1331.

Robert Koenig, Renato Renner, Sampling of min-entropy relative to quantum knowledge, arXiv:0712.4291.

Matthew Leifer, David Poulin, Quantum graphical models and belief propagation, Ann. Phys., to appear, arXiv:0708.1337

Robert Koenig, Michael M. Wolf, On exchangeable continuous variable systems, arXiv:0804.3070.

Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, Stephanie Wehner,
The quantum moment problem and bounds on entangled multi-prover games,
IEEE Conference on Computational Complexity, arXiv:0803.4373.

Panos Aliferis, John Preskill, Fault-tolerant quantum computation against biased noise, arXiv:0710.1301.

Panos Aliferis, Fred Brito, David DiVincenzo, John Preskill, Matthias Steffen, Barbara Terhal, Fault-tolerant computing with biased noise superconducting qubits, arXiv:0806.0383.

David Poulin, Yeojin Chung, On the iterative decoding of sparse quantum codes, arXiv:0801.1241.

David Poulin, Jean-Pierre Tillich, Harold Ollivier, Quantum serial turbo-codes, arXiv:0712.2888.

Austin G. Fowler, Kovid Goyal, Topological cluster state quantum computing, arXiv:0805.3202.

Lara Faoro, Alexei Kitaev, Lev B. Ioffe, Quasiparticle poisoning and Josephson current fluctuations induced by Kondo impurities, arXiv:0801.3919.

Patrick Hayden, John Preskill, Black holes as mirrors: quantum information in random subsystems, JHEP 0709, 120 (2007), arXiv:0708.4025.

David Poulin, Ersen Bilgin, Belief propagation algorithm for computing correlation functions in finite-temperature quantum many-body systems on loopy graphs, Phys. Rev. A 77, 052318 (2008), arXiv:0710.4304.

Igor Tupitsyn, Alexei Kitaev, Nikolay Prokof\'ev, Philip Stamp, Topological multicritical point in the Toric Code and 3D gauge Higgs Models, arXiv:0804.3175.

Florian Girelli, David Poulin, Quantum reference frames and deformed symmetries, Phys. Rev. D 77, 104012 (2008), arXiv:0710.4393.